

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-233771

(43)Date of publication of application : 02.09.1998

(51)Int.Cl.

H04L 9/32

G09C 1/00

(21)Application number : 09-296515

(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD
TOSHIBA CORP

(22)Date of filing : 29.10.1997

(72)Inventor : TATEBAYASHI MAKOTO
MATSUZAKI NATSUME
HIRAYAMA KOICHI

(30)Priority

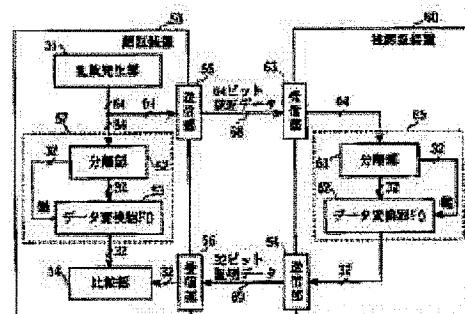
Priority number : 08290375 Priority date : 31.10.1996 Priority country : JP

(54) UNIDIRECTIONAL DATA CONVERSION DEVICE AND DEVICE AUTHENTICATION SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To execute authentication through the use of authentication data whose length is twice as much as a conventional one without increasing a circuit scale by converting first separation data based on conversion algorithm where second separation data is set to be a key and generating output data.

SOLUTION: In an authentication device 50, a separation part 52 separates the random number of 64 bits into two pieces of separation data of 64 bits. A data converter 53 converts one separation data with other separation data as the key. In a device to be verified 60, a separation part 61 separates authentication data of 64 bits into two pieces of separation data of 32 bits. A data converter 62 converts one separation data with other separation data as the key and returns it to the verification device 50. The comparison part 54 of the authentication device 50 compares two pieces of data of 32 bits, which are outputted from the data converters 53 and 62 in both devices 50 and 60. When they are matched, the authentication device 50 verifies that the device to be verified 60 is a just unit.



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平10-233771

(43) 公開日 平成10年(1998) 9月2日

(51) Int.Cl.⁸

H 0 4 L 9/32

G 0 9 C 1/00

識別記号

6 4 0

F I

H 0 4 L 9/00

G 0 9 C 1/00

6 7 5 A

6 4 0 E

審査請求 未請求 請求項の数25 O L (全 16 頁)

(21) 出願番号 特願平9-296515

(22) 出願日 平成9年(1997)10月29日

(31) 優先権主張番号 特願平8-290375

(32) 優先日 平8(1996)10月31日

(33) 優先権主張国 日本 (J P)

(71) 出願人 000005821

松下電器産業株式会社

大阪府門真市大字門真1006番地

(71) 出願人 000003078

株式会社東芝

神奈川県川崎市幸区堀川町72番地

(72) 発明者 館林 誠

大阪府門真市大字門真1006番地 松下電器産業株式会社内

(72) 発明者 松崎 なつめ

大阪府門真市大字門真1006番地 松下電器産業株式会社内

(74) 代理人 弁理士 中島 司朗

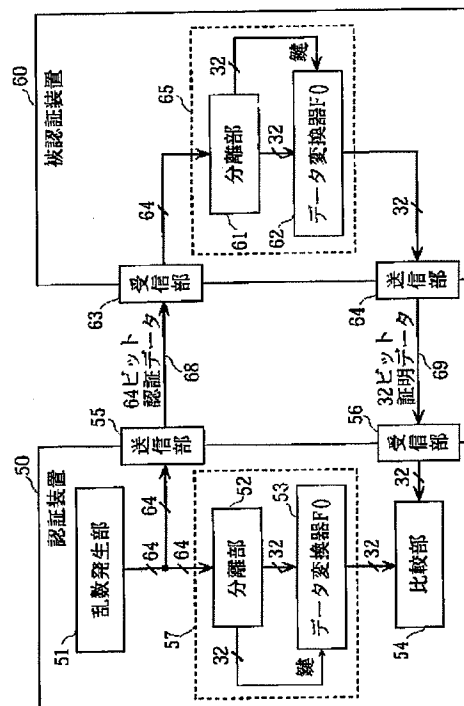
最終頁に続く

(54) 【発明の名称】 一方向データ変換装置及び機器認証システム

(57) 【要約】

【課題】 回路規模を大幅に増大することなく従来の2倍長の認証データを用いて認証を行うことができる安全性の高い機器認証システムを提供する。

【解決手段】 認証装置50は、64ビットの乱数を発生する乱数発生部51と、その乱数を認証データとして被認証装置60に送信する送信部55と、その乱数を2個の32ビットデータに分離する分離部52と、分離された一方のデータに対して、他方のデータを鍵とする秘密のアルゴリズムに基づいて変換するデータ変換器53と、送信した認証データに対して被認証装置60から返信されてきた32ビットの証明データを受信する受信部56と、その証明データとデータ変換器53からの出力データとが一致するか否かを判断する比較部54とを備え、被認証装置60も、認証装置50が備える分離部52及びデータ変換器53と同一機能の分離部61及びデータ変換器62を備える。



【特許請求の範囲】

【請求項1】 2nビットの入力データをnビットの出力データに変換する一方向データ変換装置であって、前記入力データをその入力データの相異なる桁位置のnビットずつに分離することにより、nビットの第1分離データとnビットの第2分離データを生成する分離手段と、

前記第1分離データに対して前記第2分離データを鍵とする変換アルゴリズムに基づいて変換することにより、前記出力データを生成するデータ変換手段とを備えることを特徴とする一方向データ変換装置。

【請求項2】 前記一方向データ変換装置はさらに、nビットの秘密鍵を記憶する秘密鍵記憶手段と、前記分離手段から生成された第2分離データを用いて前記秘密鍵を変更することにより、nビットの変更鍵を生成する秘密鍵変更手段とを備え、前記データ変換手段は、前記第2分離データに代えて前記変更鍵を鍵とする前記変換アルゴリズムに基づいて前記第1分離データを変換することを特徴とする請求項1記載の一方向データ変換装置。

【請求項3】 前記データ変換手段による変換は、一方向性変換であることを特徴とする請求項2記載の一方向データ変換装置。

【請求項4】 伝送路で接続された認証装置と被認証装置からなる機器認証システムであって、前記認証装置は、2nビットの乱数を発生する乱数発生手段と、前記乱数を認証データとして前記被認証装置に送信する送信手段と、前記乱数を入力データとし、秘密のアルゴリズムに基づいてnビットの出力データに変換する一方向データ変換手段と、前記認証データに対して被認証装置から返信されてきたnビットの証明データを受信する受信手段と、前記出力データと前記証明データとが一致するか否かを判断する比較手段とを備え、前記被認証装置は、前記認証装置から送信されてきた認証データを受信する受信手段と、前記認証データを入力データとし、前記アルゴリズムと同一の秘密のアルゴリズムに基づいてnビットの出力データに変換する一方向データ変換手段と、前記出力データを前記認証データに対する証明データとして前記認証装置に返信する送信手段とを備えることを特徴とする機器認証システム。

【請求項5】 前記認証装置及び前記被認証装置の一方向データ変換手段は、いずれも、前記入力データをその入力データの相異なる桁位置のnビットずつに分離することにより、nビットの第1分離データとnビットの第2分離データを生成する分離手段

と、

前記第1分離データに対して前記第2分離データを鍵とする変換アルゴリズムに基づいて変換することにより、前記出力データを生成するデータ変換手段とを有することを特徴とする請求項4記載の機器認証システム。

【請求項6】 前記認証装置及び前記被認証装置の一方向データ変換手段は、いずれもさらに、nビットの秘密鍵を記憶する秘密鍵記憶手段と、前記分離手段から生成された第2分離データを用いて前記秘密鍵を変更することにより、nビットの変更鍵を生成する秘密鍵変更手段とを有し、前記認証装置及び前記被認証装置のデータ変換手段は、前記第2分離データに代えて前記変更鍵を鍵とする前記変換アルゴリズムに基づいて前記第1分離データを変換することを特徴とする請求項5記載の機器認証システム。

【請求項7】 前記認証装置及び前記被認証装置のデータ変換手段による変換は、いずれも一方向性変換であることを特徴とする請求項6記載の機器認証システム。

【請求項8】 伝送路で接続された認証装置と被認証装置からなる機器認証システムにおける認証装置であって、

2nビットの乱数を発生する乱数発生手段と、前記乱数を認証データとして前記被認証装置に送信する送信手段と、前記乱数を入力データとし、秘密のアルゴリズムに基づいてnビットの出力データに変換する一方向データ変換手段と、前記認証データに対して被認証装置から返信されてきたnビットの証明データを受信する受信手段と、前記出力データと前記証明データとが一致するか否かを判断する比較手段とを備えることを特徴とする認証装置。

【請求項9】 前記一方向データ変換手段は、前記入力データをその入力データの相異なる桁位置のnビットずつに分離することにより、nビットの第1分離データとnビットの第2分離データを生成する分離手段と、前記第1分離データに対して前記第2分離データを鍵とする変換アルゴリズムに基づいて変換することにより、前記出力データを生成するデータ変換手段とを有することを特徴とする請求項8記載の認証装置。

【請求項10】 前記一方向データ変換手段はさらに、nビットの秘密鍵を記憶する秘密鍵記憶手段と、前記分離手段から生成された第2分離データを用いて前記秘密鍵を変更することにより、nビットの変更鍵を生成する秘密鍵変更手段とを有し、前記データ変換手段は、前記第2分離データに代えて前記変更鍵を鍵とする前記変換アルゴリズムに基づいて前記第1分離データを変換することを特徴とする請求項9

記載の認証装置。

【請求項11】 前記データ変換手段による変換は、一方向性変換であることを特徴とする請求項10記載の認証装置。

【請求項12】 前記認証装置はさらに、光ディスクからデジタル著作物を読み出す光ディスク読み出し手段と、前記比較手段によって一致すると判断された場合に、前記デジタル著作物を前記被認証装置に転送するデータ転送手段とを備えることを特徴とする請求項11記載の認証装置。

【請求項13】 伝送路で接続された認証装置と被認証装置からなる機器認証システムにおける被認証装置であって、前記認証装置から送信されてきた2nビットの認証データを受信する受信手段と、前記認証データを入力データとし、秘密のアルゴリズムに基づいてnビットの出力データに変換する一方向データ変換手段と、前記出力データを前記認証データに対する証明データとして前記認証装置に返信する送信手段とを備えることを特徴とする被認証装置。

【請求項14】 前記一方向データ変換手段は、前記入力データをその入力データの相異なる桁位置のnビットずつに分離することにより、nビットの第1分離データとnビットの第2分離データを生成する分離手段と、前記第1分離データに対して前記第2分離データを鍵とする変換アルゴリズムに基づいて変換することにより、前記出力データを生成するデータ変換手段とを有することを特徴とする請求項13記載の被認証装置。

【請求項15】 前記一方向データ変換手段はさらに、nビットの秘密鍵を記憶する秘密鍵記憶手段と、前記分離手段から生成された第2分離データを用いて前記秘密鍵を変更することにより、nビットの変更鍵を生成する秘密鍵変更手段とを有し、前記データ変換手段は、前記第2分離データに代えて前記変更鍵を鍵とする前記変換アルゴリズムに基づいて前記第1分離データを変換することを特徴とする請求項14記載の被認証装置。

【請求項16】 前記データ変換手段による変換は、一方向性変換であることを特徴とする請求項15記載の被認証装置。

【請求項17】 前記被認証装置はさらに、前記認証装置から転送されてきたデジタル著作物を受信する転送データ受信手段と、受信したデジタル著作物を映像再生する映像再生手段とを備えることを特徴とする請求項16記載の被認証装置。

【請求項18】 伝送路で接続された認証装置と被認証

装置からなる機器認証システムであって、

前記認証装置は、

2nビットの乱数を発生する乱数発生手段と、前記乱数をその乱数の相異なる桁位置のnビットずつに分離することにより、nビットの第1分離データとnビットの第2分離データを生成する分離手段と、前記第1分離データに対して前記第2分離データを暗号鍵とする暗号アルゴリズムに基づいて暗号化することにより、nビットの暗号文を生成する暗号化手段と、前記暗号文と前記第2分離データとを各ビットを混ぜることで結合し、2nビットの出力データを生成する結合手段と、

前記出力データを認証データとして前記被認証装置に送信する送信手段と、

前記認証データに対して被認証装置から返信されてきたnビットの証明データを受信する受信手段と、

前記証明データと前記第1分離データとが一致するか否かを判断する比較手段とを備え、

前記被認証装置は、

前記認証装置から送信されてきた認証データを受信する受信手段と、

受信した認証データをその認証データの相異なる桁位置のnビットずつに分離することにより、前記暗号文と同じnビットの第3分離データと前記第2分離データと同じnビットの第4分離データを生成する分離手段と、前記第3分離データに対して前記第4分離データを復号鍵とする復号アルゴリズムに基づいて復号化することにより、nビットの復号文を生成する復号化手段と、前記復号文を前記認証データに対する証明データとして前記認証装置に返信する送信手段とを備えることを特徴とする機器認証システム。

【請求項19】 前記認証装置はさらに、

nビットの秘密鍵を記憶する秘密鍵記憶手段と、

前記分離手段から生成された第2分離データを用いて前記秘密鍵を変更することにより、nビットの変更鍵を生成する秘密鍵変更手段とを備え、

前記暗号化手段は、前記第2分離データに代えて前記変更鍵を暗号鍵とする前記暗号アルゴリズムに基づいて前記第1分離データを暗号化し、

前記被認証装置はさらに、

nビットの秘密鍵を記憶する秘密鍵記憶手段と、

前記分離手段から生成された第4分離データを用いて前記秘密鍵を変更することにより、nビットの変更鍵を生成する秘密鍵変更手段とを備え、

前記復号化手段は、前記第4分離データに代えて前記変更鍵を復号鍵とする前記復号アルゴリズムに基づいて前記第3分離データを復号化することを特徴とする請求項18記載の機器認証システム。

【請求項20】 伝送路で接続された認証装置と被認証装置からなる機器認証システムにおける認証装置であつ

て、
 2nビットの乱数を発生する乱数発生手段と、
 前記乱数をその乱数の相異なる桁位置のnビットずつに
 分離することにより、nビットの第1分離データとnビ
 ットの第2分離データを生成する分離手段と、
 前記第1分離データに対して前記第2分離データを暗号
 鍵とする暗号アルゴリズムに基づいて暗号化すること
 により、nビットの暗号文を生成する暗号化手段と、
 前記暗号文と前記第2分離データとを各ビットを混ぜる
 ことで結合し、2nビットの出力データを生成する結合
 手段と、
 前記出力データを認証データとして前記被認証装置に送
 信する送信手段と、
 前記認証データに対して被認証装置から返信されてきた
 nビットの証明データを受信する受信手段と、
 前記証明データと前記第1分離データとが一致するか否
 かを判断する比較手段と
 を備えることを特徴とする認証装置。

【請求項21】 前記認証装置はさらに、
 nビットの秘密鍵を記憶する秘密鍵記憶手段と、
 前記分離手段から生成された第2分離データを用いて前
 記秘密鍵を変更することにより、nビットの変更鍵を生
 成する秘密鍵変更手段とを備え、
 前記暗号化手段は、前記第2分離データに代えて前記変
 更鍵を暗号鍵とする前記暗号アルゴリズムに基づいて前
 記第1分離データを暗号化することを特徴とする請求項
 20記載の認証装置。

【請求項22】 前記認証装置はさらに、
 光ディスクからデジタル著作物を読み出す光ディスク読
 み出し手段と、
 前記比較手段によって一致すると判断された場合に、前
 記デジタル著作物を前記被認証装置に転送するデータ転
 送手段とを備えることを特徴とする請求項21記載の認
 証装置。

【請求項23】 伝送路で接続された認証装置と被認証
 装置からなる機器認証システムにおける被認証装置であ
 って、
 前記認証装置から送信されてきた2nビットの認証デー
 タを受信する受信手段と、
 受信した認証データをその認証データの相異なる桁位置
 のnビットずつに分離することにより、nビットの第1
 分離データとnビットの第2分離データを生成する分離
 手段と、
 前記第1分離データに対して前記第2分離データを復号
 鍵とする復号アルゴリズムに基づいて復号化すること
 により、nビットの復号文を生成する復号化手段と、
 前記復号文を前記認証データに対する証明データとして
 前記認証装置に返信する送信手段とを備えることを特徴
 とする被認証装置。

【請求項24】 前記被認証装置はさらに、

nビットの秘密鍵を記憶する秘密鍵記憶手段と、
 前記分離手段から生成された第2分離データを用いて前
 記秘密鍵を変更することにより、nビットの変更鍵を生
 成する秘密鍵変更手段とを備え、
 前記復号化手段は、前記第2分離データに代えて前記変
 更鍵を復号鍵とする前記復号アルゴリズムに基づいて前
 記第1分離データを復号化することを特徴とする請求項
 23記載の被認証装置。

【請求項25】 前記被認証装置はさらに、

前記認証装置から転送されてきたデジタル著作物を受信
 する転送データ受信手段と、
 受信したデジタル著作物を映像再生する映像再生手段と
 を備えることを特徴とする請求項24記載の被認証装
 置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、一方向データ変換
 装置及びそれを用いた機器認証システムに関し、特に、
 大きなサイズの伝送データを用いて認証する技術に関す
 る。

【0002】

【従来の技術】デジタル化された文書、音声、画像、
 プログラムなどのデータをネットワークを介して通信を
 行うシステムや、前記デジタルデータを記録保存、読
 み出しするシステム等においては、前記デジタルデー
 タにアクセスしようとする者が予め許可された正当な者
 かどうかを事前に検査する必要がある。

【0003】そのために、ネットワークや記録媒体への
 データアクセスに際しては、アクセスの正当性を示すた
 めに認証手続きが用いられている。最も簡単な認証方式
 として、アクセス者からIDとパスワードを送る方式が
 ある。しかし、この方式では、伝送路を流れる他人のID
 とパスワードを盗聴等によって入手すれば簡単に不正
 な認証を行うことができるので、安全性が高いとは言え
 ない。

【0004】安全性の高い従来の機器認証システムとし
 て、一方向性関数を用いる第1の従来技術と、暗号器と
 復号器の対を用いる第2の従来技術がある。図15は、
 一方向性関数を用いた第1の従来技術に係る機器認証シ
 ステムの構成を示すブロック図である。このシステム
 は、伝送路24、25を介して接続された認証装置10
 と被認証装置20から構成される。

【0005】認証装置10は、被認証装置20を認証す
 る側の機器であり、32ビットの乱数を発生する乱数発
 生部11と、その乱数を認証データとして被認証装置20
 に送信する送信部14と、その乱数を秘密の一方向性
 関数f()に基づいて変換するデータ変換器12と、被認
 証装置20から証明データを受信する受信部15と、そ
 の証明データとデータ変換器12が生成したデータとの
 一致を比較する比較部13とから構成される。なお、認

証データとは、認証装置から被認証装置に送られるチャレンジデータであって、認証装置が被認証装置に対して自己の正当性を証明させる機会を与えるためのデータという。

【0006】一方、被認証装置20は、認証装置10に対して自己の正当性を証明する機器であり、認証装置10から送られてきた認証データを受信する受信部22と、その認証データを秘密の一方方向性関数 $f()$ に基づいて変換するデータ変換器21と、データ変換器21が生成したデータを証明データとして認証装置10に返信する送信部23とから構成される。なお、証明データとは、認証データを受信した被認証装置が自己の正当性を証明するために認証装置に返信するレスポンスデータという。

【0007】本図では、認証装置10が備えるデータ変換器12と被認証装置20が備えるデータ変換器21は同一である（同一の関数 $f()$ に基づく変換を行う）ので、乱数発生部11が発生した1個の乱数に対して、認証装置10及び被認証装置20は同一の変換を行うことから、比較部13での比較結果は一致することになる。これによって、認証装置10は「相手機器（被認証装置20）は自己が備える秘密のデータ変換器12と同一のデータ変換器を備える」と判断し、被認証装置20の正当性を認める（認証する）。

【0008】一方、比較部13での比較結果が不一致となる場合は、認証装置10は、「相手機器は自己が備える秘密のデータ変換器12と同一のデータ変換器を備えない」ことを知るので、相手機器の正当性を認めない（認証しない）。なお、本システムにおいて、乱数により認証の都度異なる認証データを用いるのは、次の理由による。

【0009】もし毎回固定の認証データを用いる場合には、それに対する毎回固定の証明データは伝送路25を一度盗聴するだけで第三者が入手可能であり、それを用いて不正な被認証装置が正当な被認証装置を装って認証させてしまうことが出来るからである。図16は、暗号器と復号器の対を用いた第2の従来技術に係る機器認証システムの構成を示すブロック図である。

【0010】第1の従来技術では、両装置10、20それぞれは同一のデータ変換器12、21を備えたが、この第2の従来技術では、両装置30、40それぞれは秘密の暗号アルゴリズム $E()$ に基づく暗号化をする暗号器32、その暗号アルゴリズム $E()$ の逆変換である秘密の復号アルゴリズム $D()$ に基づく復号化をする復号器41を備える。また、第1の従来技術では、認証データは乱数そのものであり、認証装置10は両データ変換器12、21の変換結果どうしを比較したが、この第2の従来技術では、認証装置30が送信する認証データは乱数を暗号化した暗号文であり、認証装置30は、証明データとして被認証装置40から返信される復号文と暗号化

前の元の乱数とを比較する。

【0011】この第2の従来技術においても、比較部33での比較結果が一致した場合に、認証装置30は「相手機器（被認証装置40）は自己が備える秘密の暗号器32に対応する復号器41を備える」と判断し、被認証装置40の正当性を認める（認証する）ことができる。ところで、このような従来の機器認証システムでは、認証データとそれに対応する証明データとの組合せの種類（組数）は十分に大きいことが必要とされる。

【0012】もし、不正な第三者による伝送路24、25、44、45の盗聴によって、認証データとそれに対応する正しい証明データとの組が全ての組合せについて収集され尽くされた場合には、もはや秘密のアルゴリズム $f()$ 、 $E()$ 、 $D()$ 自体が解読されたことに等しいからである。また、不正な機器が認証装置になりすまして、全てのとり得る認証データを順次に正当な被認証装置に送信し、それぞれに対する証明データを収集するという不正行為に対して防御する必要もある。

【0013】従って、このような機器認証システムにおいては、認証データと証明データとの組数は、現実的な計算機のパワーや時間内においては認証データと証明データとの全ての組合せが収集されないだけの莫大な数であることが要求される。

【0014】

【発明が解決しようとする課題】しかしながら、上述の従来の機器認証システムでは、認証データと証明データとの組数を増やすために認証データのデータ長（ビット長）を大きくしようとすると、それを入力とするデータ変換器12、21、暗号器32、復号器41の回路規模を大幅に増大しなければならないという問題点がある。

【0015】具体的には、上記従来の機器認証システムでは、認証データと証明データはそれぞれ32ビットであるので、これらの組合せは全部で2の32乗通りである。即ち、伝送路には2の32乗通りの認証データと証明データとの組合せが出現し得る。この場合、1msの時間で1つの組を伝送路上に出現させてこれを盗むことが出来るとすると、1週間もしないうちに全ての組を収集できてしまう。また、1時間そこそこで入手出来る全組数の100分の1程度のデータに基づいて正規の被認証装置になりすますることが出来る確率も極めて高い。これでは十分に安全な組数とは言えない。

【0016】このシステムの安全性を高めるためには、例えば認証データを64ビットに増やすことで上記組数を増加させればよい。しかし、そのためには少なくとも両装置が備えるデータ変換器12、21、暗号器32、復号器41の回路規模を2倍以上にする必要があり、これでは、回路規模の制約が厳しい小型・携帯型の電子機器や高速な認証手続が要求される通信機器等においては実装が困難であり、断念せざるを得ない。

【0017】そこで、本発明はかかる問題点に鑑みてな

されたものであり、従来とほぼ等しい回路規模で構成されるにも拘わらず従来の2倍長の認証データを用いて認証を行うことができる安全性の高い機器認証システム及びそのための一方データ変換装置を提供することを目的とする。

【0018】

【課題を解決するための手段】上記目的を達成するために、認証装置及び被認証装置に用いられる一方データ変換装置や暗号器・復号器は、通常、入出力データ長がともにnビットであり、両装置はnビットの共通鍵を所持して動作していることに着目し、そのような特性を有効利用することで以下の発明を考案した。

【0019】本発明は、2nビットの入力データを意味のないnビットの出力データに変換する一方データ変換装置であって、前記入力データをその入力データの相異なる桁位置のnビットずつに分離することにより、nビットの第1分離データとnビットの第2分離データを生成する分離手段と、前記第1分離データに対して前記第2分離データを鍵とする変換アルゴリズムに基づいて変換することにより、前記出力データを生成するデータ変換手段とを備える。

【0020】この一方データ変換装置は、nビットデータからnビットデータに変換する手段（データ変換手段）にビット分離するための簡単な配線等の手段（分離手段）を付加したものである。このような一方データ変換装置を備える機器認証システムの一形態は、認証装置が、2nビットの乱数を生成する乱数発生手段と、その乱数を2個のnビットの第1及び第2分離データにビット分離する分離手段と、第1分離データに対して第2分離データを鍵として変換するデータ変換手段と、その変換結果nビットと被認証装置から返信されてきた証明データnビットとが一致するか否かを判断する比較手段とを備え、一方、被認証装置が、認証装置が備える分離手段及びデータ変換手段それぞれと同じ機能の分離手段及びデータ変換手段等を備え、認証装置が発生した2nビットの乱数（認証データ）からnビットの証明データを生成し認証装置に返信する、システムである。

【0021】ここで、データ変換手段自体は一方方向性関数に基づく変換手段であってもよい。また、分離手段で生成された第2分離データを鍵としてデータ変換手段に入力する代わりに、予め記憶された秘密鍵をその第2分離データで変更し、その変更結果を鍵としてデータ変換手段に入力することもできる。また、上記一方データ変換装置を備える機器認証システムの他の形態は、暗号器と復号器とを用いるシステムであって、認証装置は、2nビットの乱数を発生する乱数発生手段と、前記乱数をその乱数の相異なる桁位置のnビットずつに分離することにより、nビットの第1分離データとnビットの第2分離データを生成する分離手段と、前記第1分離データに対して前記第2分離データを暗号鍵とする暗号アル

ゴリズムに基づいて暗号化することにより、nビットの暗号文を生成する暗号化手段と、前記暗号文と前記第2分離データとを各ビットを混ぜることで結合し、2nビットの出力データを生成する結合手段と、前記認証データに対して被認証装置から返信されてきたnビットの証明データと前記第1分離データとが一致するか否かを判断する比較手段とを備え、一方、被認証装置は、認証装置から送信されてきた認証データをその認証データの相異なる桁位置のnビットずつに分離することにより、前記暗号文と同じnビットの第3分離データと前記第2分離データと同じnビットの第4分離データを生成する分離手段と、前記第3分離データに対して前記第4分離データを復号鍵とする復号アルゴリズムに基づいて復号化することにより、認証装置に返信すべきnビットの証明データを生成する復号化手段とを備える。

【0022】ここで、上記第2分離データ（及び第4分離データ）を暗号鍵（復号鍵）として暗号器（復号器）に入力する代わりに、予め記憶された秘密鍵をその第2分離データ（及び第4分離データ）で変更し、その変更結果を暗号鍵（復号鍵）として暗号器（復号器）に入力することもできる。

【0023】

【発明の実施の形態】以下、本発明に係る機器認証システムについて図面を用いて詳細に説明する。

（実施の形態1）図1は、本発明に係る実施形態1の機器認証システムの構成を示すブロック図である。

【0024】本システムは、一方データ変換装置を用いた機器認証システムであり、伝送路68、69で接続された認証装置50と被認証装置60から構成される。認証装置50は、被認証装置60を認証する側の機器であり、乱数発生部51、一方データ変換装置57（分離部52及びデータ変換器53）、比較部54、送信部55及び受信部56を備える。

【0025】乱数発生部51は、認証に際して1個の並列64ビットの乱数を発生する。送信部55は、並列to直列変換器等であり、乱数発生部51が発生した並列64ビットの乱数を直列に変換し、認証データとして伝送路68を介して被認証装置60に送信する。一方データ変換装置57は、64ビットの入力データを秘密の変換アルゴリズムに基づいて32ビットの出力データに変換する回路であり、この回路の秘密性を確保するために1個のシリコン基板にICとして形成されており、分離部52とデータ変換器53とから構成される。

【0026】ここで、一方データ変換装置とは、任意の入力データを変換して1つの出力データを生成するが、生成された出力データからは入力データを一義的に特定できないような変換を行う装置をいう。この一方データ変換装置57は、入力データよりも少ないビット数の出力データを生成するので、一方方向性の変換を行う装置と言える。

【0027】分離部52は、図2に示されるような固定的な配線であり、乱数発生部51が発生した64ビットの乱数A0～A63を、不規則なビット配分に従って、2つの32ビットの分離データ(B0～B31とC0～C31)に分離する。つまり、これら2つの分離データは、入力された64ビットの乱数の相異なる32個の桁から構成される。

【0028】データ変換器53は、分離部52で生成された1つの32ビットの分離データC0～C31を変換対象とし、もう1つの分離データB0～B31を鍵とする変換関数F()に基づいて変換することにより、意味のない32ビットのデータを生成する論理回路である。受信部56は、直列to並列変換器等であり、送信部55が送信した認証データに対して被認証装置60から返信されてくる直列32ビットの証明データを受信し、並列に変換して比較部54に送る。

【0029】比較部54は、ラッチ回路及びコンパレータ回路等であり、データ変換器53が生成した32ビットのデータと受信部56から送られてきた32ビットの証明データとを比較し、それらが一致するか否か判断する。一致した場合は、認証装置50は被認証装置60を認証し、そうでない場合は認証しない。一方、被認証装置60は、認証装置50に対して自己の正当性を証明する機器であり、一方向データ変換装置65(分離部61及びデータ変換器62)、受信部63及び送信部64を備える。

【0030】受信部63は、直列to並列変換器等であり、認証装置50から送信されてきた直列64ビットの認証データを受信し、並列に変換して分離部61に送る。一方向データ変換装置65は、認証装置50が備える一方向データ変換装置57と同一であり、64ビットの入力データを秘密の変換アルゴリズムに基づいて32ビットの出力データに変換する回路であり、この回路の秘密性を確保するために1個のシリコン基板にICとして形成されており、分離部61とデータ変換器62とから構成される。

【0031】分離部61は、認証装置50が備える分離部52と同一であり、受信部63から送られてきた64ビットの認証データA0～A63を2つの32ビットの分離データ(B0～B31とC0～C31)に分離する。データ変換器62は、認証装置50が備えるデータ変換器53と同一であり、分離部61で生成された1つの32ビットの分離データC0～C31を変換対象とし、もう1つの分離データB0～B31を鍵とする変換関数F()に基づいて変換することにより、意味のない32ビットのデータを生成する論理回路である。

【0032】送信部64は、並列to直列変換器等であり、データ変換器62が生成した並列32ビットのデータを直列に変換し、証明データとして伝送路69を介して認証装置50に返信する。図3は、データ変換器53

(及びデータ変換器62)の詳細な構成を示すブロック図である。

【0033】このデータ変換器53(及びデータ変換器62)は、ビット置換部70、換字部71、排他的論理和部72、転字部73及びビット置換部74から構成される。ビット置換部70は、ラッチ回路及び配線等からなり、入力された32ビットデータC0～C31をビット単位で不規則に並び替える。

【0034】換字部71は、換字表を記憶するROM等からなり、ビット置換部70から出力された32ビットデータを4文字からなる文字列(先頭から8ビットずつを1文字とする)として1文字ずつ換字表を引くことで新たな4文字からなる文字列に変換する。排他的論理和部72は、図4に示されるように32個のEXORゲートからなり、換字部71から出力された32ビットデータD0～D31と分離部52(分離部61)から生成された分離データB0～B31とのビット毎の排他的論理和をとる。

【0035】転字部73は、ラッチ回路及び配線等からなり、排他的論理和部72から出力された32ビットデータE0～E31を8ビット×4文字の文字列として、文字の順番を入れ替える。ビット置換部74は、ラッチ回路及び配線等からなり、転字部73から出力された32ビットデータをビット単位で並び替える。この並び替えは、上記ビット置換部70及び転字部73のものと異なる。

【0036】このように、データ変換器53(及びデータ変換器62)は、32ビットの入力データC0～C31を意味のない32ビットの出力データに変換するが、そのときの変換アルゴリズムは排他的論理和部72に輸入される分離データB0～B31の影響を受ける。以上のように構成された本機器認証システムにおける動作は以下の通りである。

【0037】まず、認証装置50の乱数発生部51は、64ビットの乱数を生成する。送信部55はその64ビットの乱数を認証データとして被認証装置60に送信する。そして、認証装置50においては、分離部52は、その64ビットの乱数を2つの32ビットの分離データに分離し、データ変換器53は、一方の分離データに対して他方の分離データを鍵として変換する。

【0038】一方、被認証装置60においても、認証装置50と同様に、分離部61は、認証装置50から受信部63を経て送られてきた64ビットの認証データを2つの32ビットの分離データに分離し、データ変換器62は、一方の分離データに対して他方の分離データを鍵として変換し、送信部64を経て認証装置50に返信する。

【0039】最後に、認証装置50の比較部54は、両装置50、60でのデータ変換器53、62から出力された2つの32ビットデータを比較する。その結果、一

致した場合には、認証装置50は、被認証装置60が正当な機器であることを認証する。以上のように、本機器認証システムによれば、認証装置50から被認証装置60に送られる認証データは、図15に示された従来システムにおける認証データの2倍長、即ち、64ビット長であるので、認証データとそれに対応する証明データとの組数は2の64乗通りとなる。即ち、本システムでは、伝送路に出現し得る認証データと証明データとの総組数は、従来システムにおける組数(2の32乗通り)の2の32乗倍となり、不正な第三者による伝送路の盗聴に対する安全性が極めて高くなる。

【0040】ところで、本機器認証システムに必要とされるハードウェア規模は、第1の従来技術とほとんど変わらない。図15と図1を比較して分かるように、本機器認証システムの構成が従来システムと異なる主要な点は、(i)分離部52(61)が追加されていることと、(ii)データ変換器53(62)が鍵の入力ポートを備えたことである。ここで、(i)分離部52は単なる固定的な配線によって実現されており、そして、(ii)図3に示されたデータ変換器53(62)の構成要素のうち排他的論理和部72を除く構成要素70、71、73、74は、32ビットの入力データを32ビットの出力データに変換する従来システムのデータ変換器12(21)に相当すると言える。

【0041】従って、本実施形態の機器認証システムは、従来システムとほぼ等しい回路規模で構成されるにも拘わらず従来の2倍長の認証データを用いて認証を行うことができる。

(実施の形態2) 図5は、本発明に係る実施形態2の機器認証システムの構成を示すブロック図である。

【0042】本システムは、実施形態1のシステムと同様に、伝送路68、69で接続された認証装置80と被認証装置90から構成される。なお、実施形態1と同じ構成要素には同じ符号を付し、その説明は省略する。本実施形態の認証装置80及び被認証装置90が実施形態1のものとは異なる点は、それぞれが備える一方向データ変換装置83及び一方向データ変換装置93の構成要素である。

【0043】認証装置80が備える一方向データ変換装置83は、内部回路の秘密性を確保するために1個のシリコン基板にICとして形成されている点で実施形態1と同じであるが、実施形態1の分離部52及びデータ変換器53に加えて、さらに秘密鍵変更部81と秘密鍵記憶部82とを備える。秘密鍵記憶部82は、ROM等であり、1個の32ビットの秘密鍵を記憶している。

【0044】秘密鍵変更部81は、図6に示されるように32個のEXORゲートからなり、秘密鍵記憶部82から読み出した32ビットの秘密鍵と分離部52から生成された分離データB0~B31とのビット毎の排他的論理和をとり、得られた32ビットデータを鍵としてデー

タ変換器53に出力する。つまり、実施形態1の一方方向データ変換装置57では、分離部52から生成された分離データB0~B31は鍵として直接にデータ変換器53に入力されたが、本実施形態の一方方向データ変換装置83では、分離部52から生成された分離データB0~B31は秘密鍵記憶部82に記憶された秘密鍵を変更する目的(又は、秘密鍵記憶部82に記憶された秘密鍵によって変更される目的)に用いられ、変更された秘密鍵がデータ変換器53に鍵として入力される。

【0045】一方、被認証装置90が備える一方方向データ変換装置93も、認証装置80の一方方向データ変換装置83と同様に、1個のシリコン基板にICとして形成されており、実施形態1の分離部61及びデータ変換器62に加えて、さらに秘密鍵変更部91と秘密鍵記憶部92とから構成される。秘密鍵記憶部92は、認証装置80の秘密鍵記憶部82と同一であり、秘密鍵変更部91は、認証装置80の秘密鍵変更部81と同一である。

【0046】以上のように構成された本機器認証システムによれば、実施形態1のシステムと同様に、従来システムとはほぼ等しい回路規模で構成されるにも拘わらず従来の2倍長の認証データを用いて認証を行うことができる。つまり、本実施形態の一方方向データ変換装置83の構成は、従来のデータ変換器12に分離部52と秘密鍵変更部81とを追加した構成に等しいと言える。それは、本実施形態の秘密鍵記憶部82とデータ変換器53とからなる回路セット、即ち、固定的な秘密鍵で32ビットデータを変換する回路セットは、外部からの鍵に依存することなく固定的な変換アルゴリズムに基づいて32ビットデータを変換する従来システムのデータ変換器12に相当すると言えるからである。

【0047】従って、本実施形態の一方方向データ変換装置83は、従来のデータ変換器12に対して、単なる固定的な配線である分離部52と32個のEXORゲートからなる秘密鍵変更部81という、わずかな回路が追加されているに過ぎないと言える。このことは、被認証装置90が備える一方方向データ変換装置93についても同様である。

【0048】但し、実施形態1と比較し、本実施形態の機器認証システムは、分離部52(61)で生成された分離データが直接ではなく変化を受けた後にデータ変換器53(62)への鍵として入力されているので、その変化分だけ安全性は高くなっている。なお、上記実施形態1、2では、一方方向データ変換装置57、65、83、97は64ビットの入力データに対してビット分離をした後にビット置換等の変換アルゴリズムに基づいて32ビットの出力データを生成したが、本発明はこのようなビット数や変換アルゴリズムに限定されるものではない。

【0049】例えば、120ビットの入力データを56ビットの分離データと64ビットの分離データに分離

し、56ビットの分離データを暗号鍵として64ビットの分離データをデータ暗号化規格(DES)に従って暗号化してもよい。また、上記実施形態1、2では、データ変換器53、62自体は、可逆な変換器(出力データと鍵とから元の入力データに復元する逆変換が存在するような変換をする変換器)であったが、一方向性変換器(出力データと鍵とから元の入力データに復元する逆変換が存在しないような不可逆な変換をする変換器)であってもよい。

【0050】例えば、データ変換器53(62)の排他的論理和部72を構成する32個のEXORゲートのうち少なくとも1個をANDゲート又はORゲートに置き換えることによって、そのデータ変換器53(62)は一方向性変換器となるが、そのような構成であっても、機器認証システムとして成立する。上記実施形態1、2では、データ変換器53及び62は、いずれも同じ方向の変換(2つの分離データから出力データを生成する変換)にのみ用いられているので、逆変換が存在する必要がないからである。

(実施の形態3)図7は、本発明に係る実施形態3の機器認証システムの構成を示すブロック図である。

【0051】本システムは、第2の従来技術の如く、暗号器と復号器の対を用いた機器認証システムであり、かつ、実施形態2の変形例であり、伝送路68、69で接続された認証装置180と被認証装置190から構成される。なお、実施形態2と同じ構成要素には同じ符号を付し、その説明は省略する。本実施形態の認証装置180の構成が実施形態2の認証装置80と異なる点は、実施形態2の認証装置80が備える構成要素51、83、54~56に加えて、さらに結合部181を備えることである。なお、データ変換器53は、実施形態2のものと同一であるが、本実施形態では、暗号器(その逆変換である復号器が存在し、かつ、本機器認証システム(被認証装置190)で用いられている)として用いている。

【0052】結合部181は、図8に示されるような固定的な配線であり、分離部52から秘密鍵変更部81に入力された32ビットの分離データB0~B31と、データ変換器53が出力した32ビットデータ(暗号文X0~X31)とを、不規則に各ビットを混ぜて並べることにより、1個の64ビットデータ(認証データY0~Y63)に結合し送信部55に送る。この結合部181は、秘密性を確保するために、一方向データ変換装置83の構成要素52、53、81、82と共に1個のシリコン基板にICとして形成されている。

【0053】一方、被認証装置190は、一方向データ変換装置193、受信部63及び送信部64を備える点で実施形態2と同じであるが、一方向データ変換装置193の構成要素が異なる。つまり、一方向データ変換装置193は、1個のシリコン基板にICとして形成され

た秘密鍵変更部91、秘密鍵記憶部92、分離部191及びデータ逆変換器192から構成されるが、これらのうち、分離部191とデータ逆変換器192は本実施形態に固有のものである。

【0054】分離部191は、図9に示されるような固定的な配線であり、受信部63から送られてくる64ビットの認証データY0~Y63を、認証装置180が備える結合部181によるビット結合の逆変換に相当するビット配分に従って、元の32ビットの暗号文X0~X31と32ビットの分離データB0~B31とに分離する。データ逆変換器192は、認証装置180が備えるデータ変換器(暗号器)53に対応する復号器であり、分離部191で生成された32ビットの暗号文X0~X31を変換対象とし、もう1つの分離データB0~B31を鍵とする逆変換関数F-1()に基づいて変換することにより、元の32ビットの分離データC0~C31に復号する。

【0055】図10は、データ逆変換器192の詳細な構成を示すブロック図である。データ逆変換器192は、ビット置換部199、転字部198、排他的論理和部197、換字部196及びビット置換部195から構成され、これらは、それぞれ、図3に示されたデータ変換器53のビット置換部74、転字部73、排他的論理和部72、換字部71、ビット置換部70の逆変換を行うものに等しい。なお、排他的論理和部197は、EXORゲート自体の性質より、排他的論理和部72と同一の構成(32個のEXORゲート)を備える。

【0056】以上の構成によれば、結合部181と分離部191、データ変換器53とデータ逆変換器192は、それぞれ逆変換の関係にあり、かつ、秘密鍵記憶部82と秘密鍵記憶部92、秘密鍵変更部81と秘密鍵変更部91は、それぞれ同一である。従って、データ逆変換器192に入力される暗号文はデータ変換器53が出力した暗号文に等しく、かつ、データ逆変換器192に入力される鍵はデータ変換器53に入力された鍵に等しいことから、データ逆変換器192が出力する復号文はデータ変換器53に入力された平文、即ち、分離部52が生成した32ビットの分離データC0~C31に等しくなる。

【0057】よって、認証装置180の比較部54は、乱数発生部51が発生した1個の乱数について分離部52から入力される分離データと、その乱数に基づいて生成された認証データに対して被認証装置190から返信されたきた証明データとが一致すると判定するので、認証装置180は被認証装置190を認証することができる。

【0058】以上のように、本機器認証システムと図16に示された第2の従来技術とを比較して分かるように、本機器認証システムによれば、わずかなハードウェア(分離部52、191、秘密鍵変更部81、91、結合部181等)を追加しただけで、伝送路68、69に

出現し得る認証データを証明データとの総組数は2の64乗通り、すなわち従来の2の32乗倍に増加している。つまり、多くの回路を必要とする暗号器及び復号器は従来と同じ32ビット対応を使用しているにも拘わらず、従来よりも第三者の盗聴に対する安全性は飛躍的に向上されている。

【0059】なお、本実施形態では、暗号器53は、実施形態2のデータ変換装置53と同一であったが、本発明はこれに限定されない。暗号器53としてDESに準拠した暗号器を用い、復号器192として対応する復号器を用いてもよい。また、本実施形態は実施形態2の一方方向データ変換装置を用いたシステムを暗号器と復号器とを用いるシステムに変形した例であったが、実施形態1を同様に變形することもできる。つまり、認証装置180においては、分離部52からの分離データB0~B31を直接に暗号器53の暗号鍵として入力し、一方、被認証装置190においても、分離部191からの分離データB0~B31を直接に復号器192の復号鍵として入力してもよい。

【0060】さらに、上記実施形態1~3では、ほとんどの構成要素は論理回路で実現されたが、汎用のマイクロプロセッサとプログラムとの組み合わせによるソフトウェアで実現することも可能である。その場合の「回路規模」とは、そのソフトウェアのコードサイズや、それを収納するPROMの記憶容量を意味する。(具体的な通信システムへの適応例) 以上のように、本発明に係る機器認証システムは、回路規模が小さいにも拘らず大きなサイズの認証データを扱うことができる。従って、本機器認証システムは、小型で、かつ、正当な機器同士での通信のみが許可されるような高い安全性の要求される通信システムに好適である。

【0061】図11は、本発明に係る機器認証システムの具体的な通信システムへの適用例を示す図であり、映画等のデジタル著作物の映像再生システムの概観を示す。このシステムは、認証装置である光ディスクドライブ装置110と被認証装置である映像再生装置111とそれらを接続するSCSIケーブル116等からなる。光ディスクドライブ装置110は、映像再生装置111を認証した後に、光ディスク115から読み出した映像データを映像再生装置111に転送し、そこで映像再生するシステムである。

【0062】図12は、光ディスクドライブ装置110の構成を示すブロック図である。光ディスクドライブ装置110は、装置全体の制御を行うMPU124と、映像再生装置111との通信インターフェースであるSCSIコントローラ121と、光ヘッド125を制御して光ディスク115から映像データを読み出し制御する読み出し制御部122と、上述の実施形態における一方方向データ変換装置57、83、結合部181等を内蔵する暗号化IC123とからなり、映像再生装置111は正当

な機器であると認証した場合にのみ光ディスク115に記録された圧縮映像データを読み出してSCSIケーブル116を介して映像再生装置111に転送する。

【0063】図13は、光ディスクドライブ装置110の内部に実装される回路基板120の概観を示す図である。暗号化IC123は、1個のシリコン基板に形成されたLSIであり、プラスチックでモールドされたフラットパッケージの形状をしている。図14は、映像再生装置111の構成を示すブロック図である。

【0064】映像再生装置111は、装置全体の制御を行うMPU131と、光ディスクドライブ装置110との通信インターフェースであるSCSIコントローラ130と、上述の実施形態の一方方向データ変換装置65、93、193等を内蔵する暗号化IC132と、受信した映像データの伸長を行うMPEGデコーダ133と、伸長された映像データをアナログ映像信号に変換してCRT112及びスピーカ114に映像出力するAV信号処理部134とから構成される。

【0065】光ディスクドライブ装置110の内部に実装される回路基板の概観は、図13に示されるものとほぼ同様である。本発明に係る機器認証システムをこのような映像再生システムに適用することで、コンパクトな回路であるのにも拘らず、光ディスク115に記録されたデジタル著作物が不正な装置によってコピー等されることが従来よりも極めて困難となり、デジタル著作物の著作権がより強力に保護される。

【0066】

【発明の効果】以上の説明から明らかなように、本発明に係る一方方向データ変換装置は、2nビットの入力データを意味のないnビットの出力データに変換する一方方向データ変換装置であって、前記入力データをその入力データの相異なる桁位置のnビットずつに分離することにより、nビットの第1分離データとnビットの第2分離データを生成する分離手段と、前記第1分離データに対して前記第2分離データを鍵とする変換アルゴリズムに基づいて変換することにより、前記出力データを生成するデータ変換手段とを備える。

【0067】この一方方向データ変換装置は、nビットデータからnビットデータに変換する手段(データ変換手段)にビット分離するための簡単な配線等の手段(分離手段)を付加したものである。従って、このような一方方向データ変換装置を認証装置及び被認証装置それぞれが備えることで、従来とほぼ等しい回路規模で構成されるにも拘わらず従来の2倍長の認証データを用いて認証を行うことができる安全性の高い機器認証システムが実現される。

【0068】つまり、nビットの認証データ及び証明データを用いて認証する従来の機器認証システムの構成に対してわずかなハードウェアを追加するだけで、2nビットの認証データとnビットの証明データとを用いて認

証する機器認証システム、即ち、認証データと証明データのとり得る組数が2の n 乗通りから2の $2n$ 乗通り(2の n 乗倍)に増加された安全性の高い機器認証システムが実現される。

【0069】このような一方データ変換装置を備える機器認証システムの形態は、認証装置が、 $2n$ ビットの乱数を生成する乱数発生手段と、その乱数を2個の n ビットの第1及び第2分離データにビット分離する分離手段と、第1分離データに対して第2分離データを鍵として変換するデータ変換手段と、その変換結果 n ビットと被認証装置から返信されてきた証明データ n ビットとが一致するか否かを判断する比較手段とを備え、一方、被認証装置が、認証装置が備える分離手段及びデータ変換手段それぞれと同じ機能の分離手段及びデータ変換手段等を備え、認証装置が発生した $2n$ ビットの乱数(認証データ)から n ビットの証明データを生成し認証装置に返信する、システムである。

【0070】ここで、データ変換手段自体は一方性関数に基づく変換手段であってもよい。また、分離手段で生成された第2分離データを鍵としてデータ変換手段に入力する代わりに、予め記憶された秘密鍵をその第2分離データで変更し、その変更結果を鍵としてデータ変換手段に入力することもできる。これによって、データ変換手段自体の解読が困難となり、また、一方データ変換装置のアルゴリズムが複雑化されるので、システムの安全性はさらに高まる。

【0071】また、上記一方データ変換装置を備える機器認証システムの他の形態は、暗号器と復号器とを用いるシステムであって、認証装置は、 $2n$ ビットの乱数を発生する乱数発生手段と、前記乱数をその乱数の相異なる桁位置の n ビットずつに分離することにより、 n ビットの第1分離データと n ビットの第2分離データを生成する分離手段と、前記第1分離データに対して前記第2分離データを暗号鍵とする暗号アルゴリズムに基づいて暗号化することにより、 n ビットの暗号文を生成する暗号化手段と、前記暗号文と前記第2分離データとを各ビットを混ぜることで結合し、 $2n$ ビットの出力データを生成する結合手段と、前記認証データに対して被認証装置から返信されてきた n ビットの証明データと前記第1分離データとが一致するか否かを判断する比較手段とを備え、一方、被認証装置は、認証装置から送信されてきた認証データをその認証データの相異なる桁位置の n ビットずつに分離することにより、前記暗号文と同じ n ビットの第3分離データと前記第2分離データと同じ n ビットの第4分離データを生成する分離手段と、前記第3分離データに対して前記第4分離データを復号鍵とする復号アルゴリズムに基づいて復号化することにより、認証装置に返信すべき n ビットの証明データを生成する復号化手段とを備える。

【0072】ここで、上記第2分離データ(及び第4

分離データ)を暗号鍵(復号鍵)として暗号器(復号器)に入力する代わりに、予め記憶された秘密鍵をその第2分離データ(及び第4分離データ)で変更し、その変更結果を暗号鍵(復号鍵)として暗号器(復号器)に入力することもできる。これによって、基本的な構成要素は n ビット対応の回路規模であるにも拘らず、即ち、認証装置及び被認証装置それぞれは n ビット対応の暗号器及び復号器を備えるにも拘らず、 $2n$ ビットの認証データと n ビットの証明データを扱う安全性の高い機器認証システムが実現される。

【0073】以上のように、本発明によって、認証に用いる一方データ変換装置や暗号器・復号器の規模をほとんど増大させることなく、認証データと証明データの総組数は2の n 乗倍に増大するため、毎回の認証時に伝送路に出現する変換前後の伝送データを不正な第三者が1組ずつ観測して収集することで全ての組について知り尽くすことが極めて困難となり不正な認証が防止される。

【0074】よって、本発明により、わずかなハードウェアを追加するだけで、極めて解読が困難で安全性の高い認証システムが構築され、その実用性は大きい。

【図面の簡単な説明】

【図1】本発明に係る実施形態1の機器認証システムの構成を示すブロック図である。

【図2】同機器認証システムの分離部52(61)の詳細な構成を示す図である。

【図3】同機器認証システムのデータ変換器53(及びデータ変換器62)の詳細な構成を示すブロック図である。

【図4】同データ変換器53(62)の排他的論理和部72の詳細な構成を示す図である。

【図5】本発明に係る実施形態2の機器認証システムの構成を示すブロック図である。

【図6】同機器認証システムの秘密鍵変更部81(91)の詳細な構成を示す図である。

【図7】本発明に係る実施形態3の機器認証システムの構成を示すブロック図である。

【図8】同機器認証システムの結合部181の詳細な構成を示す図である。

【図9】同機器認証システムの分離部191の詳細な構成を示す図である。

【図10】同機器認証システムのデータ逆変換器192の詳細な構成を示すブロック図である。

【図11】本発明に係る機器認証システムの具体的な通信システムへの適用例を示す図である。

【図12】同通信システムにおける光ディスクドライブ装置110(認証装置)の構成を示すブロック図である。

【図13】同光ディスクドライブ装置110の内部に実装される回路基板120の概観を示す図である。

【図14】同通信システムにおける映像再生装置111（被認証装置）の構成を示すブロック図である。

【図15】一方向性関数を用いた第1の従来技術に係る機器認証システムの構成を示すブロック図である。

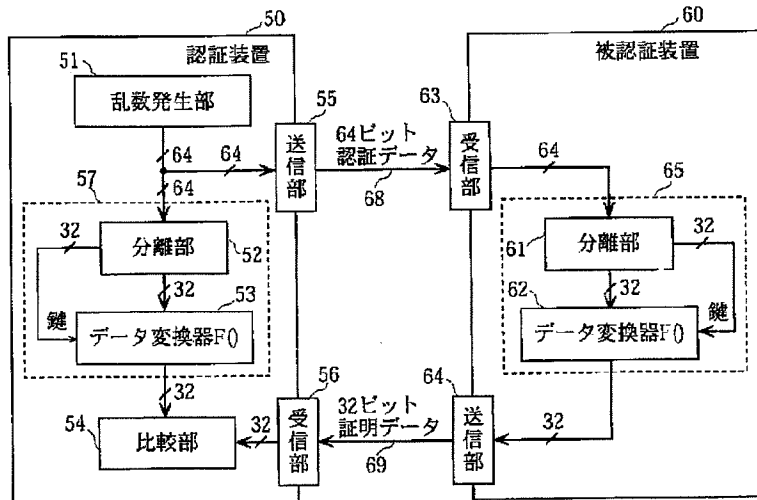
【図16】暗号器と復号器の対を用いた第2の従来技術に係る機器認証システムの構成を示すブロック図である。

【符号の説明】

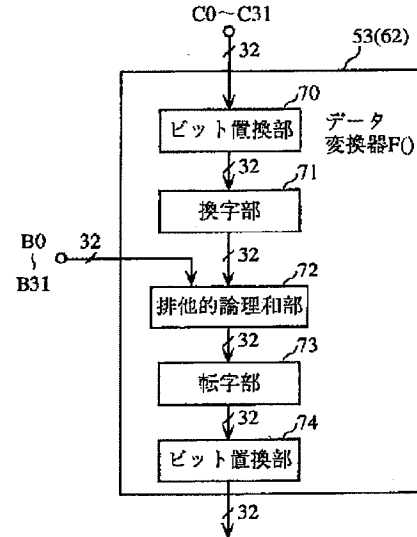
50、80、180 認証装置
51 乱数発生部
52 分離部
53 データ変換器
54 比較部
55 送信部
56 受信部
57 一方向データ変換装置
60、90、190 被認証装置

61 分離部
62 データ変換器
63 受信部
64 送信部
65 一方向データ変換装置
68 伝送路
69 伝送路
81 秘密鍵変更部
82 秘密鍵記憶部
10 83 一方向データ変換装置
91 秘密鍵変更部
92 秘密鍵記憶部
93 一方向データ変換装置
181 結合部
191 分離部
192 データ逆変換器
193 一方向データ変換装置

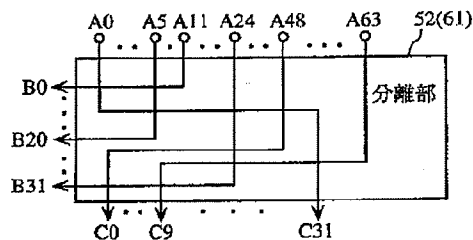
【図1】



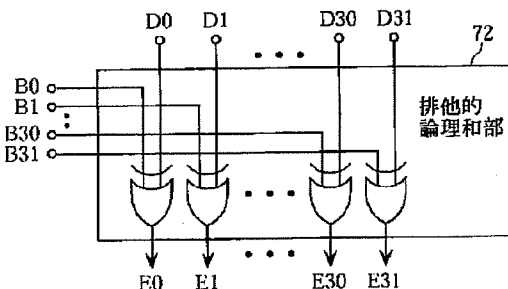
【図3】



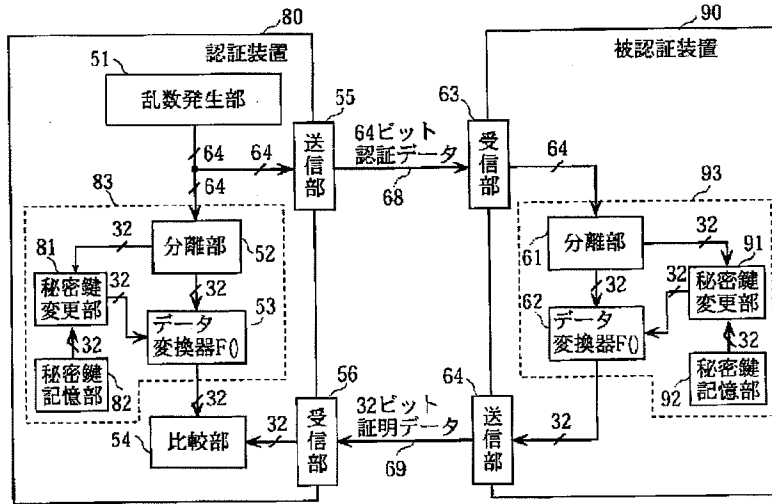
【図2】



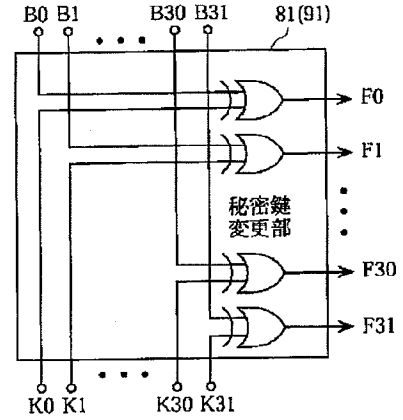
【図4】



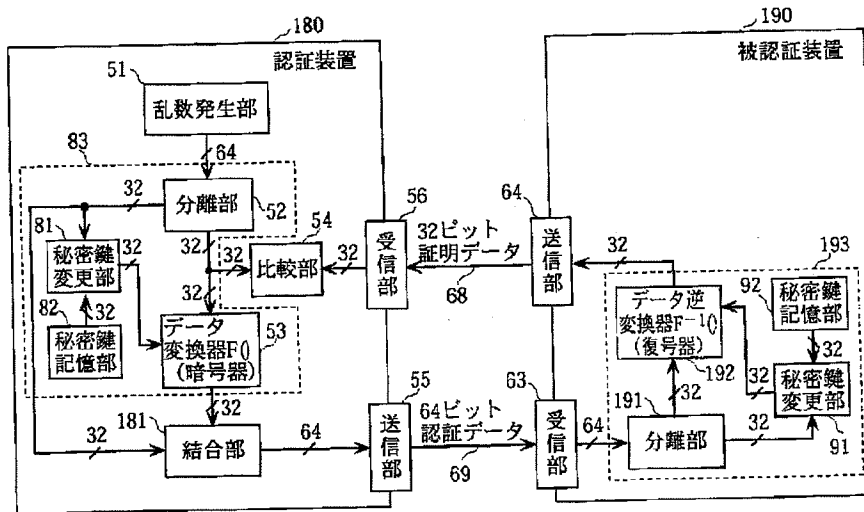
【図5】



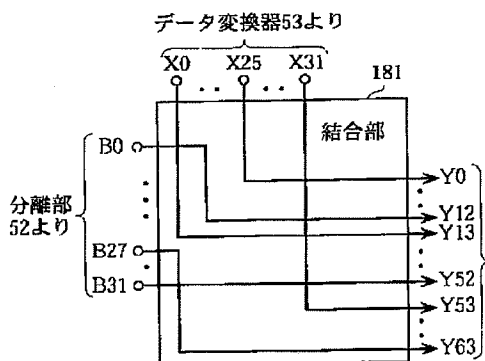
【図6】



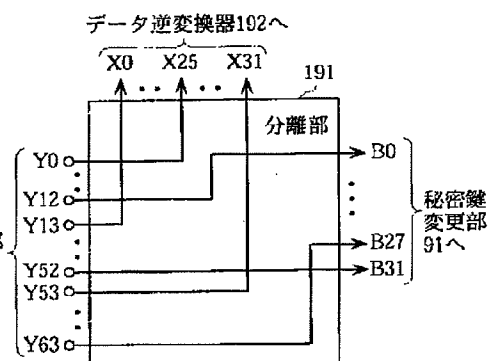
【図7】



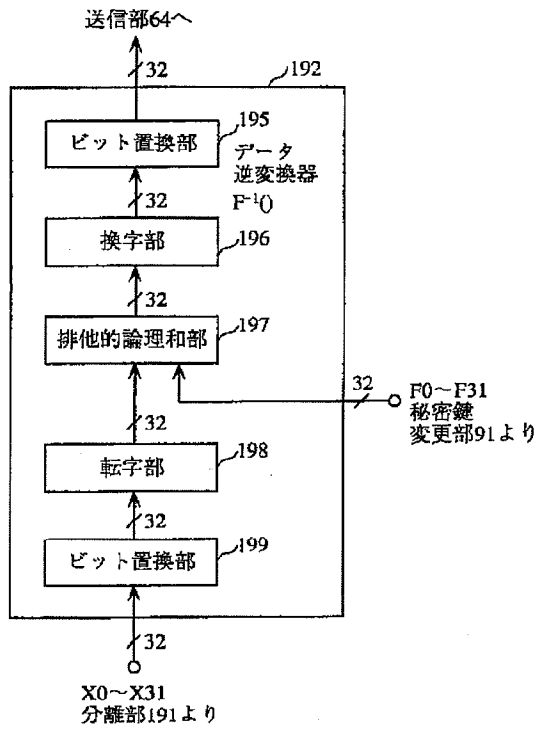
【図8】



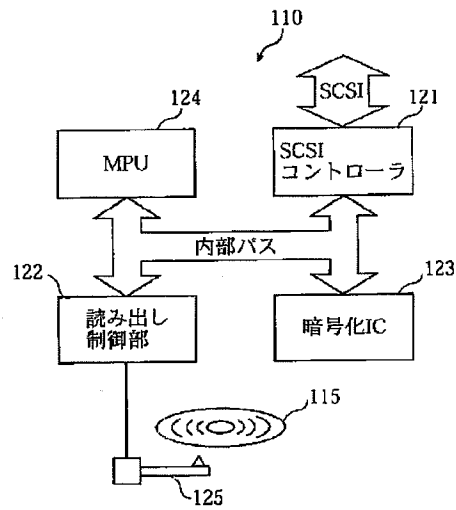
【図9】



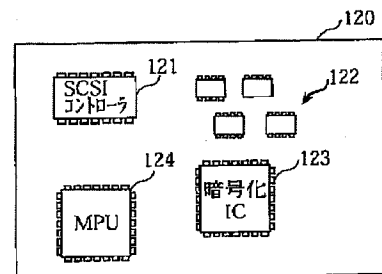
【図10】



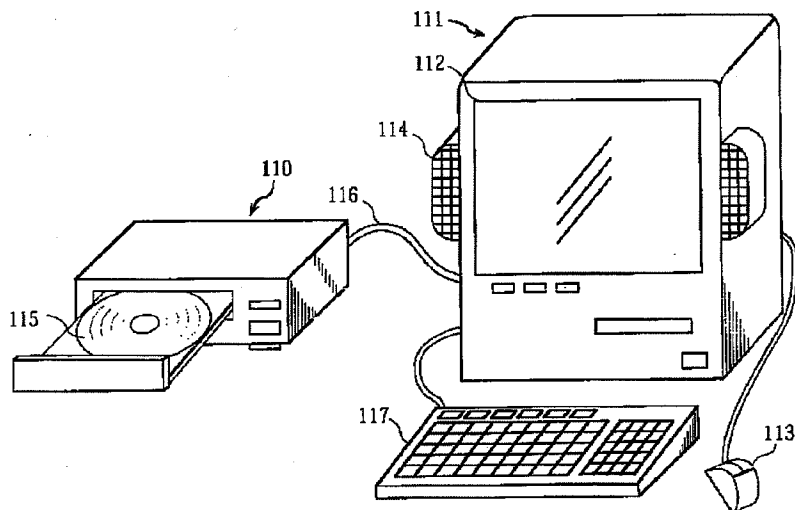
【図12】



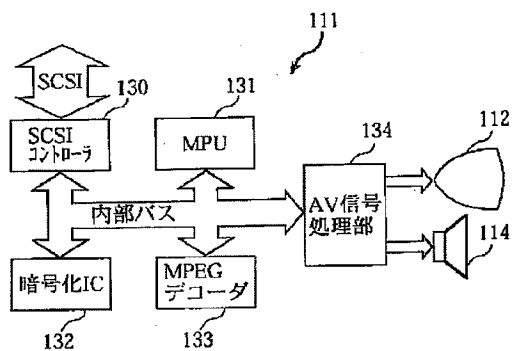
【図13】



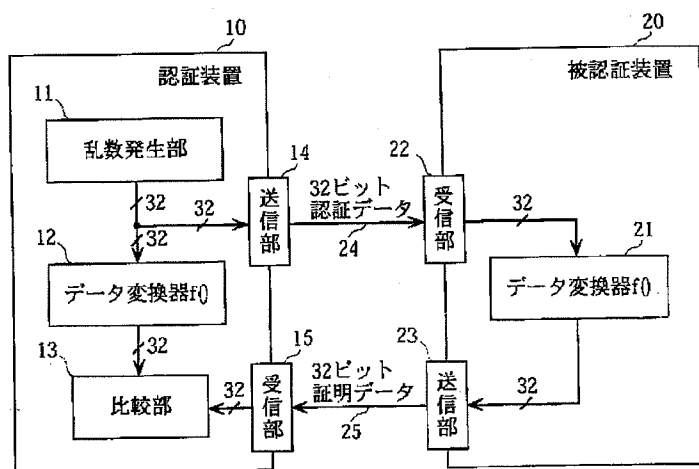
【図11】



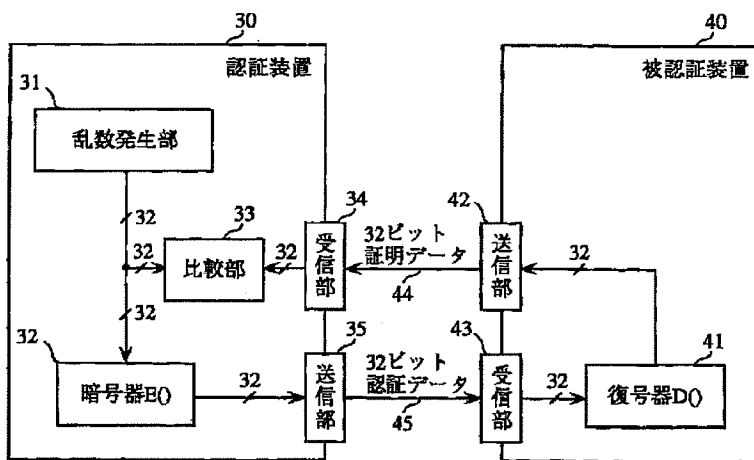
【図14】



【図15】



【図16】



フロントページの続き

(72)発明者 平山 康一

神奈川県川崎市幸区柳町70番地 株式会社
東芝柳町工場内